Cyber Counterintelligence

Counterintelligence/Open Source Symposium

17 September 2009

Threat

"the growing connectivity between information systems, the Internet, and other infrastructures creates opportunities for attackers to disrupt telecommunications, electrical power, energy pipelines, refineries, financial networks, and other critical infrastructures."

DNI Blair, March 10, 2009, Annual Threat Assessment of the Intelligence Community for the Senate Armed Services Committee

Thoughts from the China's Military

"An adversary wishing to destroy the United States only has to mess up the computer systems of its banks by high-tech means. This would disrupt and destroy the U.S. ECONOMY"

People's Liberation Daily, 1996

Threats

Industry estimates IP loss due to data theft as high as $1 trillion in 2008 ***(source; McAfee)***

In January 2009

- One in ~257 emails contained malware
- One in ~369 emails comprised a phishing attack
- 1208 new malicious websites were identified each day (contain malware, are phishing sites) ***(source: Symantec)***

The Threat is Real and Growing

Cyber threat is multi-dimensional:

- **Insider threat:** Unauthorized use or access to information, systems, and networks by otherwise trusted agents (employees)
- **Close/expanded access:** Gaining access to information or systems via deployment of technology in proximity to the target.
- **Remote (network) access:** Accessing target information and/or systems through network-based technical means
- **Exploitation of the vendor/supply chain:** Gaining advantage, control, and/or access to systems and the information they contain through manipulation by cooperative/witting vendors or unilaterally at any point in the supply chain between the manufacturer and end user.

The USG needed to build upon a "Mission Bridging" Strategic Framework addressing these Multiple Threat Vectors

Comprehensive National Cyber Initiative

- In May 2007, the DNI established a National Cyber Study Group (NCSG) consisting of six working groups to address the threat posed to U.S. computer networks for disruption and exploitation.
- In July 2007, the White House Communications Systems and Cybersecurity Policy Coordinating Committee assumed oversight and subsequently developed a set of twelve initiatives and seven enabling activities.
- In October 2007, the President approved these recommendations.
- In January 2008, the President signed NSPD-54/HSPD-23 for Cybersecurity to direct Dept/Agencies for execution.

“…cybersecurity will be designated as one of my key management priorities.. .”

- Remarks by President Obama on

Securing our Nation’s Cyber Infrastructure,

29 May 2009

Creation of the Cyber CI Plan

- **Directed by NSPD-54/HSPD-23 in January 2008 to develop a government-wide Cyber CI Plan (CNCI-6)**
  - Builds on the 2007 *National Counterintelligence Strategy of the United States.*

Cyber Counterintelligence

"Counterintelligence, by any means, where a significant target or tool of the adversarial activity is a computer, computer network, embedded processor or controller, or the information thereon."

(The United States Government-Wide Cyber Counterintelligence Plan, 2008)

Cyber CI Plan

- Detect, deter, disrupt, and mitigate internal and external threats through counterintelligence means.
- Strengthen collaboration and information sharing among security, law enforcement, and counterintelligence elements to enhance capabilities.

Cyber CI Plan

- Conduct all-source CI analysis in support of the Cyber CI mission. Primary focus is on development of a strategic cyber damage or impact assessment methodology.

- Establish/expand Cyber CI education/awareness programs and workforce development to integrate counterintelligence equities into all aspects of cyber operations and analysis.

Cyber CI Plan

- ★Mitigate supply chains threats
  - Hardware/Software
  - Identify and protect *critical national assets*
  - Trusted foundries?
  - Technical solutions?

Challenges

- ★ Bridging CI and Cybersecurity worlds within Agencies and across the USG
- ★ Sharing CI information at the lowest classification possible to enable USG and private sector to maximize response to cyber threats
- ★ CI workforce recruitment and training

Future

- “Cyber Czar”
  - Elevation of management to White House level
- Focus on “Cyberspace Policy Review” recommendations
  - Education and awareness
  - Private sector and Government partnerships
  - Effective information sharing and incident response
  - Encourage innovation

    (Cyberspace Policy Review “Assuring a Trusted and Resilient Information and Communications Infrastructure”)